Formal Verification of Nonlinear Inequalities with Taylor Interval Approximations

Alexey Solovyev, Thomas Hales

University of Pittsburgh

NASA Formal Methods Symposium, May 15, 2013

Main Results

- Implementation of a tool in HOL Light for a complete formal verification of nonlinear inequalities.
- The tool can verify general multivariate polynomial and non-polynomial inequalities in the form

$$\forall \mathbf{x} \in \mathbb{R}^n, \mathbf{x} \in D \implies f(\mathbf{x}) < 0.$$

  where $D = \{(x_1, \ldots, x_n) \mid a_i \leq x_i \leq b_i\} = [\mathbf{a}, \mathbf{b}]$.
- Formal verification of nonlinear inequalities in the Flyspeck project (a formal proof of the Kepler conjecture).
- The tool can be downloaded from the Flyspeck project repository at `http://code.google.com/p/flyspeck/downloads/list`

Examples of Verified Inequalities

General Inequalities

- A polynomial inequality

$$-\frac{1}{\sqrt{3}} \le x \le \sqrt{2},\ -\sqrt{\pi} \le y \le 1$$
$$\implies x^2y - xy^4 + y^6 + x^4 - 7 > -7.17995$$

- A non-polynomial inequality

$$0 \le x \le 1 \implies \arctan(x) - \frac{x}{1 + 0.28x^2} < 0.005$$

Examples of Verified Inequalities

Flyspeck Inequalities

Define
$$\Delta(x_1,\ldots,x_6) = x_1x_4(-x_1+x_2+x_3-x_4+x_5+x_6) + x_2x_5(x_1-x_2+x_3+x_4-x_5+x_6) + x_3x_6(x_1+x_2-x_3+x_4+x_5-x_6) - x_2x_3x_4 - x_1x_3x_5 - x_1x_2x_6 - x_4x_5x_6,$$

$$\Delta_y(y_1,\ldots,y_6) = \Delta(y_1^2,\ldots,y_6^2), \quad \Delta_4 = \frac{\partial\Delta}{\partial x_4},$$

$$\mathrm{dih}\,(y_1,\ldots,y_6) = \frac{\pi}{2} - \mathrm{arctan}_2\left(\sqrt{4y_1^2\Delta_y(y_1,\ldots,y_6)}, -\Delta_4(y_1^2,\ldots,y_6^2)\right).$$

Let $D = \{\mathbf{x} \in \mathbb{R}^6 \mid 2 \le x_i \le 2.52\}$, then

$$\forall \mathbf{x}.\ \mathbf{x} \in D \implies \mathrm{dih}\,(\mathbf{x}) < 1.893,$$

$$\forall \mathbf{x}.\ \mathbf{x} \in D \implies \Delta_y(\mathbf{x}) > 0.$$

HOL Light

- The system is implemented in the OCaml programming language.
- A very simple logical core (less than 700 lines of code).
- Contains a large library of formalized theorems.
- John Harrison, the developer of HOL Light, contributed a lot to the Flyspeck project by proving many important foundational theorems in HOL Light.

The Kepler Conjecture and the Flyspeck Project

Theorem

No packing of congruent balls in Euclidean three dimensional space has density greater than that of the face-centered cubic packing.

The maximum density is $\pi/\sqrt{18} \approx 0.74$

- In 1611, Johannes Kepler formulated the conjecture.
- In 1831, Gauss established a special case of the conjecture.
- In 1953, Fejes Tóth formulated a general strategy to confirm the Kepler conjecture.
- In 1998, Thomas Hales solved the conjecture (published in 2006).
- In 2003, Hales launched the Flyspeck project.

The Flyspeck Project

- The goal of the Flyspeck project is a complete formal verification of the Kepler conjecture.
- The name of the project comes from the matching of the pattern F*P*K (Formal Proof of Kepler) against the English dictionary.
- There are 985 nonlinear inequalities in the Flyspeck project.
- Involve arctangents, arccosines, square roots, rational expressions.
- 6–9 variables. Most inequalities contain 6 variables.
- Each inequality has the following form:

$$\forall \mathbf{x} \in [\mathbf{a}, \mathbf{b}] \implies f_1(\mathbf{x}) < 0 \vee \ldots \vee f_k(\mathbf{x}) < 0.$$

- The official website: `http://code.google.com/p/flyspeck/`

Overview of Verification Methods

Methods

- Interval arithmetic.
- Interval arithmetic with Taylor approximations.
- Bernstein polynomials.
- Subdivision of domains.

Overview of Verification Methods

Some existing formalizations

- Univariate inequalities in PVS based on Taylor interval arithmetic: Marc Daumas, David Lester, and César Muñoz, *Verified real number calculations: A library for interval arithmetic*
- Multivariate polynomial inequalities in PVS based on Bernstein polynomials.
  - César Muñoz and Anthony Narkawicz, *Formalization of a Representation of Bernstein Polynomials and Applications to Global Optimization*
  - Roland Zumkeller's optimization program Sergei `http://code.google.com/p/sergei/`

Interval Arithmetic

Example

Prove $x_1^2 + x_2^2 \geq 0$ when $x_1, x_2 \in [0, 2] \times [0, 1]$.
Interval computations yield:

$$0 \leq x_1^2 \leq 4, \quad 0 \leq x_2^2 \leq 1,$$

$$0 \leq x_1^2 + x_2^2 \leq 5$$

and the inequality follows.

Dependency problem

Compute an interval for $x - x$ when $0 \leq x \leq 2$.
We get $-2 \leq x - x \leq 2$, meanwhile the best answer is $0 \leq x - x \leq 0$.
Intervals become wide very quickly.

Interval Arithmetic with Taylor Approximations

$$f(x) = f(y) + \sum_{i=1}^{k} \frac{f^{(k)}(y)(x-y)^k}{k!} + error.$$

To find an interval bound of $f(x)$ on a domain $a \leq x \leq b$, find interval bounds of $f(y), f'(y), \ldots, f^{(k)}(y)$ and an interval bound of the error term for all $a \leq x \leq b$.

Example

$$f(x) = x - x^2, \quad 0.1 \leq x \leq 0.3, \quad y = 0.2$$

We find $f(y) = 0.16$, $f'(y) = 0.6$, and $f''(x) = -2$ for all x.

$$0.16 - 0.6 \times 0.1 - \frac{1}{2} \times 0.1^2 \times 2 \leq f(x) \leq 0.16 + 0.6 \times 0.1 + \frac{1}{2} \times 0.1^2 \times 2,$$

Taylor approximation: $0.09 \leq x - x^2 \leq 0.23$ when $0.1 \leq x \leq 0.3$.
Interval arithmetic: $0.01 \leq x - x^2 \leq 0.29$.
Exact result: $0.09 \leq x - x^2 \leq 0.21$.

Domain Subdivision

- To improve the accuracy of estimates (in all methods above), the domain of interest can be subdivided into smaller domains and estimates are computed on each subdomain.
- If a strict inequality $f(\mathbf{x}) < r$ holds on a domain

$$D = [\mathbf{a}, \mathbf{b}] = \{a_i \leq x_i \leq b_i\},$$

then all method presented above will prove this inequality if $D = \cup D_i$ is divided into sufficiently small subdomains D_i (conditions on f are also required, like $f \in C^2(D)$).

Example (Interval Arithmetic)

Prove $x^2 > -10^{-10}$ when $x \in [-1, 2]$.
Interval arithmetic gives: $x \in [-1, 2] \implies -2 \leq x \leq 4$.
Divide the domain into two subdomains: $[-1, 2] = [-1, 0] \cup [0, 2]$.
Interval arithmetic: $x \in [-1, 0] \implies 0 \leq x \leq 1$, $x \in [0, 2] \implies 0 \leq x \leq 4$, and the inequality follows.

Main Estimate

Consider a rectangular domain

$$D = \{a_i \le x_i \le b_i \mid i = 1, \ldots, n\} = [\mathbf{a}, \mathbf{b}] \subset \mathbb{R}^n.$$

Take $\mathbf{y} \in D$ and find $\mathbf{w}$ s.t. $\mathbf{w} \ge 0$ and $|\mathbf{x} - \mathbf{y}| \le \mathbf{w}$ (componentwise).
Denote partial derivatives of f as f_i, second partial derivatives as f_{ij}.

Theorem

Suppose $f \in C^2(D)$ and $\left|f_{ij}(\mathbf{x})\right| \le d_{ij}$ for all $\mathbf{x} \in D$. Then

$$\forall \mathbf{x}.\ \mathbf{x} \in D \implies \left| f(\mathbf{x}) - f(\mathbf{y}) - \sum_{i=1}^{n} |f_i(\mathbf{y})| w_i \right| \le \frac{1}{2} \sum_{i,j=1}^{n} d_{ij} w_i w_j.$$

To compute an interval bound of f on D, it is required to compute intervals for $f(\mathbf{y})$, $f_i(\mathbf{y})$ $(i = 1, \ldots, n)$, $f_{ij}(\mathbf{x})$ $(i, j = 1, \ldots, n,\ \mathbf{x} \in D)$.

Verification Procedure

Goal: verify $f(\mathbf{x}) < 0$ on $D = [\mathbf{a}, \mathbf{b}]$.

1 $y := (\mathbf{a} + \mathbf{b})/2$. Find $\mathbf{w} \geq 0$ s.t. $\mathbf{y} - \mathbf{a} \leq \mathbf{w}$ and $\mathbf{b} - \mathbf{y} \leq \mathbf{w}$.

2 Find an upper bound u of f with the Taylor approximation.

3 If $u < 0$, then done. Otherwise [4]

4 Find j s.t. $w_j \geq w_i$ for all i. Let $D^{(1)} = [\mathbf{a}, \mathbf{c}^{(1)}]$ and $D^{(2)} = [\mathbf{c}^{(2)}, \mathbf{b}]$ where $c_i^{(1)} = b_i$, $i \neq j$, and $c_j^{(1)} = y_j$; $c_i^{(2)} = a_i$, $i \neq j$, and $c_j^{(2)} = y_j$.

5 Repeat the procedure for $D = D^{(1)}$ and for $D = D^{(2)}$.

Monotonicity Arguments

Decreasing function

If $f_k(\mathbf{x}) \leq 0$ on $[\mathbf{a}, \mathbf{b}]$, then it is sufficient to verify $f(\mathbf{x}) < 0$ on $[\mathbf{a}, \mathbf{c}]$ where $c_i = b_i$, $i \neq k$, $c_k = a_k$.

Increasing function

If $f_k(\mathbf{x}) \geq 0$ on $[\mathbf{a}, \mathbf{b}]$, then it is sufficient to verify $f(\mathbf{x}) < 0$ on $[\mathbf{c}, \mathbf{b}]$ where $c_i = a_i$, $i \neq k$, $c_k = b_k$.

Formalization Overview

- Formal Taylor intervals.
- Solution certificates.
  - Computed informally.
  - An input for a formal verification procedure.
- Formal verification procedures.

Formal Taylor Interval: Definitions

$$\mathrm{CD}(\mathbf{x}, \mathbf{z}, \mathbf{y}, \mathbf{w}) \iff (\forall i,\ 1 \le i \le n \implies x_i \le y_i \le z_i \ \wedge\ \max\{y_i - x_i, z_i - y_i\} \le w_i)\,.$$

$$\mathrm{LA}(f, \mathbf{y}, f^{lo}, f^{hi}, [(f_1^{lo}, f_1^{hi}); \ldots; (f_n^{lo}, f_n^{hi})]) \iff \left(f^{lo} \le f(\mathbf{y}) \le f^{hi} \ \wedge\ (\forall i,\ f_i^{lo} \le \frac{\partial f}{\partial x_i}(\mathbf{y}) \le f_i^{hi})\right).$$

$$\mathrm{B}_2(f, \mathbf{x}, \mathbf{z}, [[f_{1,1}^{lo}, f_{1,1}^{hi}]; [f_{2,1}^{lo}, f_{2,1}^{hi}; f_{2,2}^{lo}, f_{2,2}^{hi}]; \ldots; [f_{n,1}^{lo}, f_{n,1}^{hi}; \ldots; f_{n,n}^{lo}, f_{n,n}^{hi}]]) \iff \left(\forall \mathbf{p},\ \mathbf{p} \in [\mathbf{x}, \mathbf{z}] \implies \left(\forall i\ j,\ j \le i \implies f_{i,j}^{lo} \le \frac{\partial^2 f}{\partial x_j \partial x_i}(\mathbf{p}) \le f_{i,j}^{hi}\right)\right).$$

$$\mathrm{TI}(f, \mathbf{x}, \mathbf{z}, \mathbf{y}, \mathbf{w}, f^{lo}, f^{hi}, d_{list}, dd_{list}) \iff \mathrm{CD}(\mathbf{x}, \mathbf{z}, \mathbf{y}, \mathbf{w}) \wedge\ f \in C^2([\mathbf{x}, \mathbf{z}]) \ \wedge\ \mathrm{LA}(f, \mathbf{y}, f^{lo}, f^{hi}, d_{list}) \ \wedge\ \mathrm{B}_2(f, \mathbf{x}, \mathbf{z}, dd_{list}).$$

Formal Taylor Interval: Operations

Implemented operations

- Addition: $+$
- Subtraction: $-$
- Multiplication: $\times$
- Division: $/$
- Square root: $\sqrt{}$
- Arctangent: $\arctan$
- Arccosine: $\arccos$

Formal Taylor Interval: Bounds

Theorem

$$
\begin{aligned}
&\mathrm{TI}(f, \mathbf{x}, \mathbf{z}, \mathbf{y}, \mathbf{w}, f^{lo}, f^{hi}, [d_1], [[dd_{1,1}]; [dd_{2,1}; dd_{2,2}]]) \\
&\quad \wedge\ w_1|d_1| + w_2|d_2| \le b \\
&\quad \wedge\ w_1(w_1|dd_{1,1}|) + w_2(w_2|dd_{2,2}| + 2w_1|dd_{2,1}|) \le e \\
&\quad \wedge\ b + 2^{-1}e \le a \ \wedge\ l \le f^{lo} - a \ \wedge\ f^{hi} + a \le h \\
&\quad \Longrightarrow\ \big(\forall \mathbf{p},\ \mathbf{p} \in [\mathbf{x}, \mathbf{z}] \implies f(\mathbf{p}) \in [l, h]\big).
\end{aligned}
$$

$$
\Big|d_i\Big| = \Big|(f_i^{lo}, f_i^{hi})\Big| = \max\{-f_i^{lo}, f_i^{hi}\}.
$$

Analogous results hold for other dimensions and for bounds of partial derivatives.

Solution Certificate

A simplified OCaml definition of the solution certificate

```
Certificate =
| Result_pass
| Result_glue of int * Certificate * Certificate
| Result_mono of bool * int * Certificate
```

No information about subdomains is explicitly given: subdomains can be reconstructed from a certificate.

Result_pass

Verification procedure

- Find a formal Taylor interval for the current subdomain.
- Formally compute the upper bound for the Taylor interval.
- Verify that the upper bound is less than 0.
- Return a theorem of the form

$$\vdash \forall \mathbf{x}.\ \mathbf{x} \in D \Longrightarrow f(\mathbf{x}) < 0.$$

Result_glue (j, Cert1, Cert2)

Verification procedure

- Subdivide the current domain along the j-th coordinate.
- Verify the inequality for the first subdomain using Cert1.
- Verify the inequality for the second subdomain using Cert2.
- Glue the results with the theorem

$$\begin{aligned}
\vdash &(\forall i.\ i \neq j \implies \mathbf{c}_i^{(1)} = \mathbf{b}_i \wedge \mathbf{c}_i^{(2)} = \mathbf{a}_i) \\
&\wedge \mathbf{c}_j^{(1)} = \mathbf{y}_j \wedge \mathbf{c}_j^{(2)} = \mathbf{y}_j \\
&\wedge \left(\forall \mathbf{x}.\ \mathbf{x} \in [\mathbf{a}, \mathbf{c}^{(1)}] \implies f(\mathbf{x}) < 0\right) \\
&\wedge (\forall \mathbf{x}.\ \mathbf{x} \in [\mathbf{c}^{(2)}, \mathbf{b}] \implies f(\mathbf{x}) < 0) \\
&\implies (\forall \mathbf{x}.\ \mathbf{x} \in [\mathbf{a}, \mathbf{b}] \implies f(\mathbf{x}) < 0)
\end{aligned}$$

Result_mono (increasing, j, Cert)

Verification procedure

- Reduce the dimension of the current domain.
- Verify the inequality for the new domain with Cert.
- Formally estimate bounds of the j-th partial derivative on the full domain.
- Apply the theorem (for the increasing case):

$$
\begin{aligned}
&\vdash f \in C^2([\mathbf{a}, \mathbf{b}]) \wedge (\forall i.\ i \neq j \Longrightarrow \mathbf{c}_i = \mathbf{a}_i) \wedge \mathbf{c}_j = \mathbf{b}_j \\
&\quad \wedge (\forall \mathbf{y}.\ \mathbf{y} \in [\mathbf{a}, \mathbf{b}] \Longrightarrow 0 \leq f_j(\mathbf{y})) \\
&\quad \wedge (\forall \mathbf{x}.\ \mathbf{x} \in [\mathbf{c}, \mathbf{b}] \Longrightarrow f(\mathbf{x}) < 0) \\
&\quad \Longrightarrow (\forall \mathbf{x}.\ \mathbf{x} \in [\mathbf{a}, \mathbf{b}] \Longrightarrow f(\mathbf{x}) < 0)
\end{aligned}
$$

Example: A Simple Polynomial Inequality

Verify $x_1^3 + x_2 > -1.1$ when $(x_1, x_2) \in [-1, 1] \times [0, 1] = [(-1, 0), (1, 1)]$.
Equivalent problem: $-1.1 - (x_1^3 + x_2) < 0$ when $(x_1, x_2) \in [-1, 1] \times [0, 1]$.

Solution Certificate

```
Mono 2 [
  Glue 1 [
    Glue 1 [
      Pass (on [-1,-0.5] x [0,0]);
      Pass (on [-0.5,0] x [0,0])
    ];
  Pass (on [0,1] x [0,0])
]
```

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.
Mono 2 $\vdash \forall p.\ p \in [-1,1] \times [0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \leq 0$
Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.
Mono 2 $\vdash \forall p.\ p \in [-1,1] \times [0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \leq 0$
Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.

Mono 2 $\vdash \forall p.\ p \in [-1,1] \times [0,1] \implies \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \leq 0$

Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

- Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$
  - Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(-0.5,0),(-0.75,0),(0.25,0)\big)$
    - Pass $\vdash \forall p.\ p \in [-1,-0.5] \times [0,0] \implies -1.1 - (p_1^3 + p_2) \leq -0.06874$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.
Mono 2 $\vdash \forall p.\ p \in [-1,1] \times [0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \leq 0$
Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(-0.5,0),(-0.75,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-1,-0.5] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \leq -0.06874$

Domain 2: $\vdash \mathrm{CD}\big((-0.5,0),(0,0),(-0.25,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-0.5,0] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \leq -0.94367$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.

Mono 2 $\vdash \forall p.\ p \in [-1,1] \times [0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \le 0$

Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(-0.5,0),(-0.75,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-1,-0.5] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.06874$

Domain 2: $\vdash \mathrm{CD}\big((-0.5,0),(0,0),(-0.25,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-0.5,0] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.94367$

Result $\vdash \forall p.\ p \in [-1,0] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) < 0$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.

Mono 2 $\vdash \forall p.\ p \in [-1,1] \times [0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \le 0$

Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(-0.5,0),(-0.75,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-1,-0.5] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.06874$

Domain 2: $\vdash \mathrm{CD}\big((-0.5,0),(0,0),(-0.25,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-0.5,0] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.94367$

Result $\vdash \forall p.\ p \in [-1,0] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) < 0$

Domain 2: $\vdash \mathrm{CD}\big((0,0),(1,0),(0.5,0),(0.5,0)\big)$

Pass $\vdash \forall p.\ p \in [0,1] \times [0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.1$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.

Mono 2 $\vdash \forall p.\ p \in [-1,1]\times[0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \le 0$

Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(-0.5,0),(-0.75,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-1,-0.5]\times[0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.06874$

Domain 2: $\vdash \mathrm{CD}\big((-0.5,0),(0,0),(-0.25,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-0.5,0]\times[0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.94367$

Result $\vdash \forall p.\ p \in [-1,0]\times[0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) < 0$

Domain 2: $\vdash \mathrm{CD}\big((0,0),(1,0),(0.5,0),(0.5,0)\big)$

Pass $\vdash \forall p.\ p \in [0,1]\times[0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) \le -0.1$

Result $\vdash \forall p.\ p \in [-1,1]\times[0,0] \Longrightarrow -1.1 - (p_1^3 + p_2) < 0$

Example: A Simple Polynomial Inequality

Initial domain: $\vdash \mathrm{CD}\big((-1,0),(1,1),(0,0.5),(1,0.5)\big)$.

Mono 2 $\vdash \forall p.\ p \in [-1,1]\times[0,1] \Longrightarrow \frac{\partial}{\partial x_2}(\lambda x. -1.1 - (x_1^3 + x_2))\ p \le 0$

Restricted domain: $\vdash \mathrm{CD}\big((-1,0),(1,0),(0,0),(1,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(0,0),(-0.5,0),(0.5,0)\big)$

Glue 1 Domain 1: $\vdash \mathrm{CD}\big((-1,0),(-0.5,0),(-0.75,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-1,-0.5]\times[0,0] \Longrightarrow -1.1-(p_1^3+p_2) \le -0.06874$

Domain 2: $\vdash \mathrm{CD}\big((-0.5,0),(0,0),(-0.25,0),(0.25,0)\big)$

Pass $\vdash \forall p.\ p \in [-0.5,0]\times[0,0] \Longrightarrow -1.1-(p_1^3+p_2) \le -0.94367$

Result $\vdash \forall p.\ p \in [-1,0]\times[0,0] \Longrightarrow -1.1-(p_1^3+p_2) < 0$

Domain 2: $\vdash \mathrm{CD}\big((0,0),(1,0),(0.5,0),(0.5,0)\big)$

Pass $\vdash \forall p.\ p \in [0,1]\times[0,0] \Longrightarrow -1.1-(p_1^3+p_2) \le -0.1$

Result $\vdash \forall p.\ p \in [-1,1]\times[0,0] \Longrightarrow -1.1-(p_1^3+p_2) < 0$

Final Result $\vdash \forall p.\ p \in [-1,1]\times[0,1] \Longrightarrow -1.1-(p_1^3+p_2) < 0$.

Performance Tests: Polynomial Inequalities

Test Polynomial Problems

Prove $m < p(x)$ for all $x \in [a, b]$.

- **schwefel**: $(x_1 - x_2^2)^2 + (x_2 - 1)^2 + (x_1 - x_3^2)^2 + (x_3 - 1)^2$, $m = -5.8806 \times 10^{-10}$, $[a, b] = [(-10, -10, -10), (10, 10, 10)]$
- **lv**: $x_1 x_2^2 + x_1 x_3^2 + x_1 x_4^2 - 1.1 x_1 + 1$, $m = -20.801$, $[a, b] = [(-2, -2, -2, -2), (2, 2, 2, 2)]$
- **magnetism**: $x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2 + 2x_5^2 + 2x_6^2 + 2x_7^2 - x_1$, $m = -0.25001$, $[a, b] = [(-1, -1, -1, -1, -1, -1, -1), (1, 1, 1, 1, 1, 1, 1)]$
- **heart**: $-x_1 x_6^3 + 3x_1 x_6 x_7^2 - x_3 x_7^3 + 3x_3 x_7 x_6^2 - x_2 x_5^3 + 3x_2 x_5 x_8^2 - x_4 x_8^3 + 3x_4 x_8 x_5^2 - 0.9563453$, $m = -1.7435$, $[a, b] = [(-0.1, 0.4, -0.7, -0.7, 0.1, -0.1, -0.3, -1.1), (0.4, 1, -0.4, 0.4, 0.2, 0.2, 1.1, -0.3)]$

Performance Tests: Polynomial Inequalities

Table: Test Results for Polynomial Inequalities in PVS and HOL Light

Inequality ID	# variables	PVS Bernstein (s)	HOL Light (s)
schwefel	3	10.23	26.329
lv	4	4.75	1.875
magnetism	7	160.44	7.007
heart	8	79.68	17.298

Performance Tests: Flyspeck Inequalities

Inequality ID	formal (s)	informal (s)
2485876245a	5.530	0
4559601669b	4.679	0
4717061266	27.1	0
5512912661	8.860	0.002
6096597438a	0.071	0
6843920790	2.824	0.002
SDCCMGA b	9.012	0.006
7067938795	431	0.070
5490182221	1726	0.375
3318775219	17091	8.000

Optimization Strategies

Implemented optimization techniques

- Efficient natural number arithmetic which works with arbitrary base representations of numerals in HOL Light.
- Formal floating-point and interval arithmetic for real numbers in HOL Light.
- Cached arithmetic.
- Adaptive arithmetic precision.

Future work

- Verification of groups of inequalities (on common subdomains).
- Do not recompute bounds of second partial derivative on small subdomains.
- Optimized evaluation of formal Taylor intervals.

Thank you!